Working Together to Build Confidence

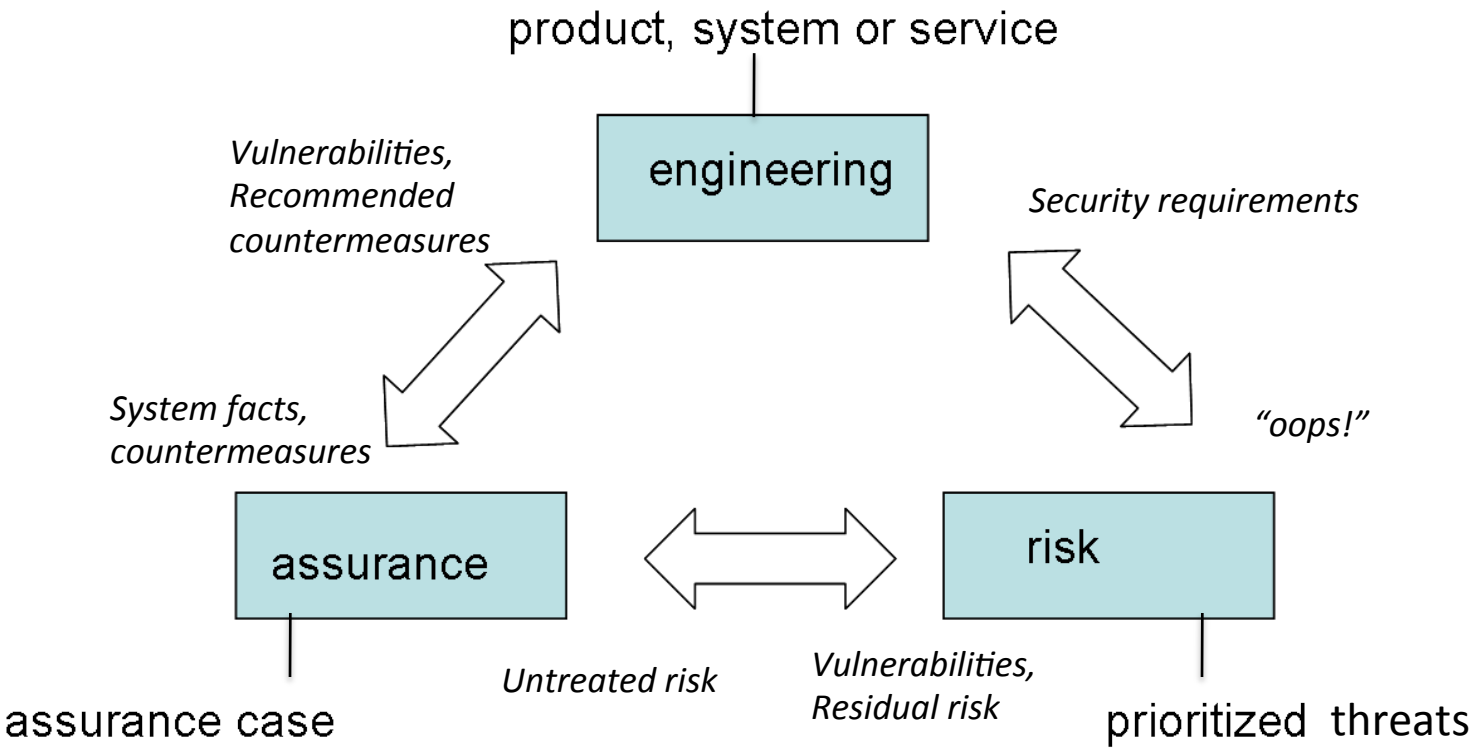
Understanding Risk through Software Assurance

Nikolai Mansourov
CTO, KDM Analytics

nick@kdmanalytics.com

Sept 19 2012

Engineering, Assurance and Risk



Assurance: How do we know that countermeasures are effective against the known threats ?

Understanding risk THROUGH assurance

- Assurance = residual risk + confidence
  - Risk factors:
    - Understanding threats,
    - Severity of their consequence,
    - Likelihood of their occurrence
    - Untreated [or *Environmental*] risk
    - Vulnerability
    - Countermeasures
    - Residual risk

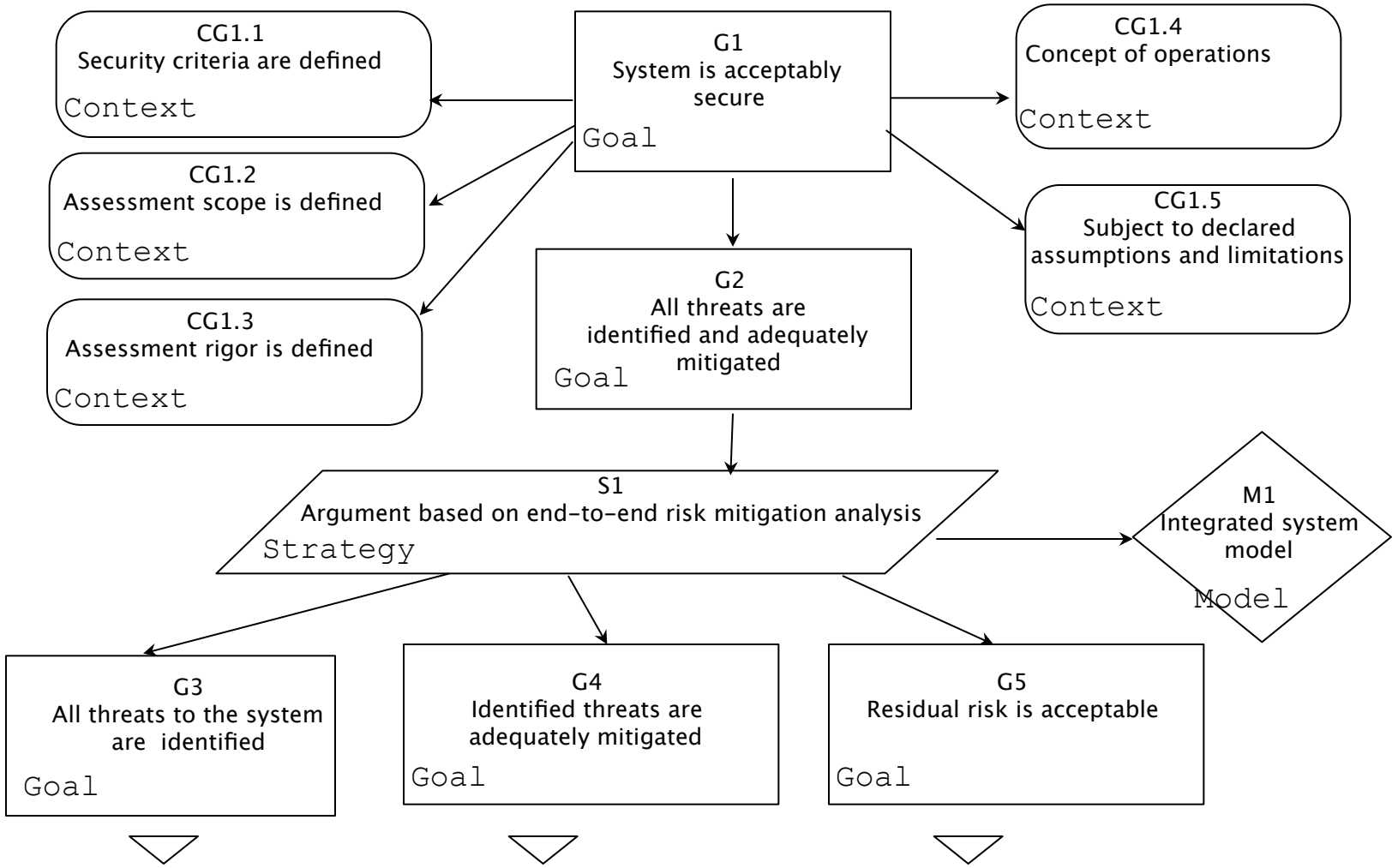
risk

risk mitigation

End-to-end risk mitigation argument

Assurance focuses on vulnerability [and risk mitigation] and helps understand residual risk

End-to-end risk mitigation argument



Understanding risk FOR assurance

- Assurance = residual risk + confidence
  - Risk factors:
    - Understanding threats,
    - Severity of their consequence,
    - Likelihood of their occurrence
    - Untreated [or *Environmental*] risk
    - Vulnerability
    - Countermeasures
    - Residual risk

Confidence ?

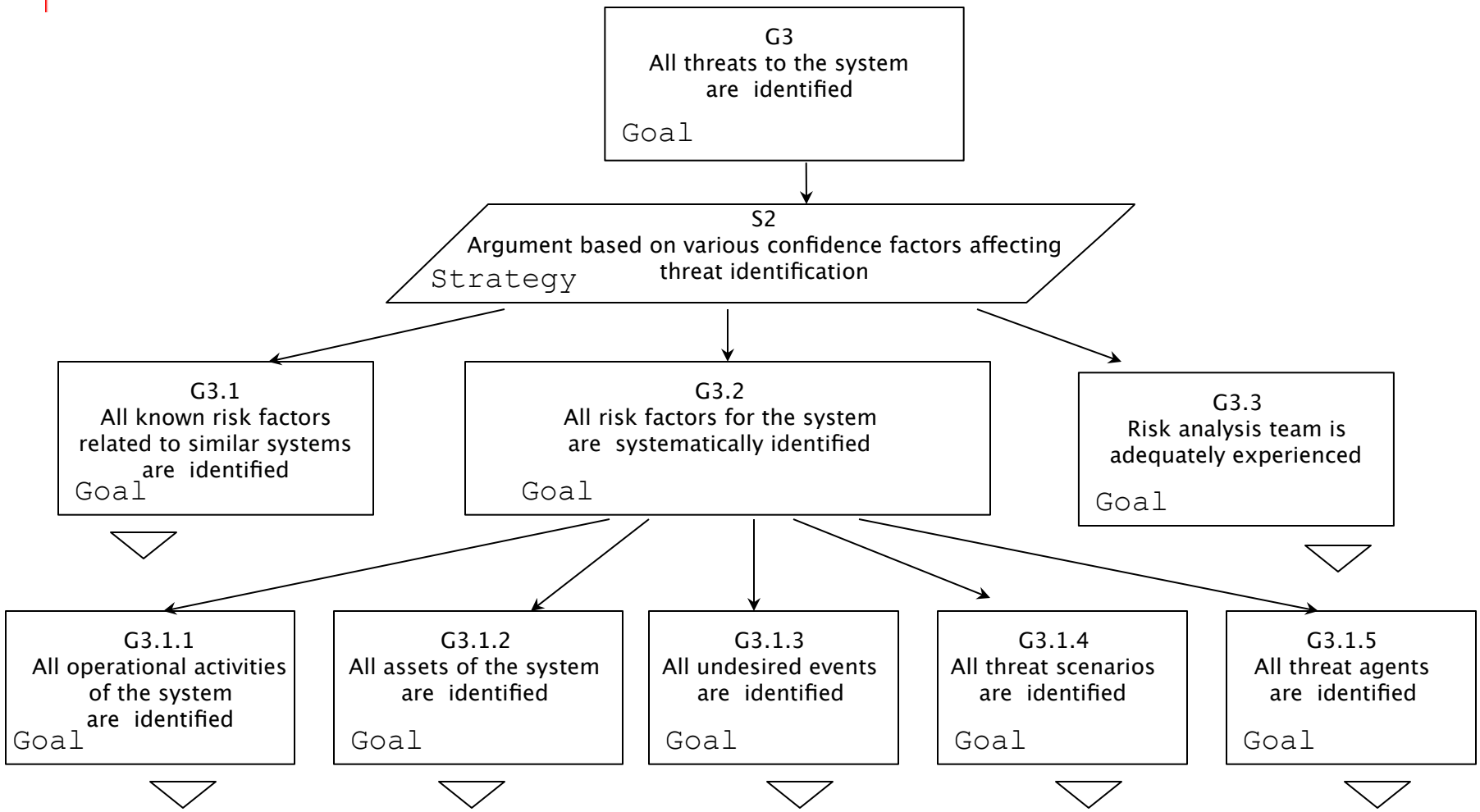
Confidence ?

Confidence ?

In order to have confidence we must first understand untreated risk

Failing to understand the ENTIRE risk …

Understanding ENTIRE risk for assurance



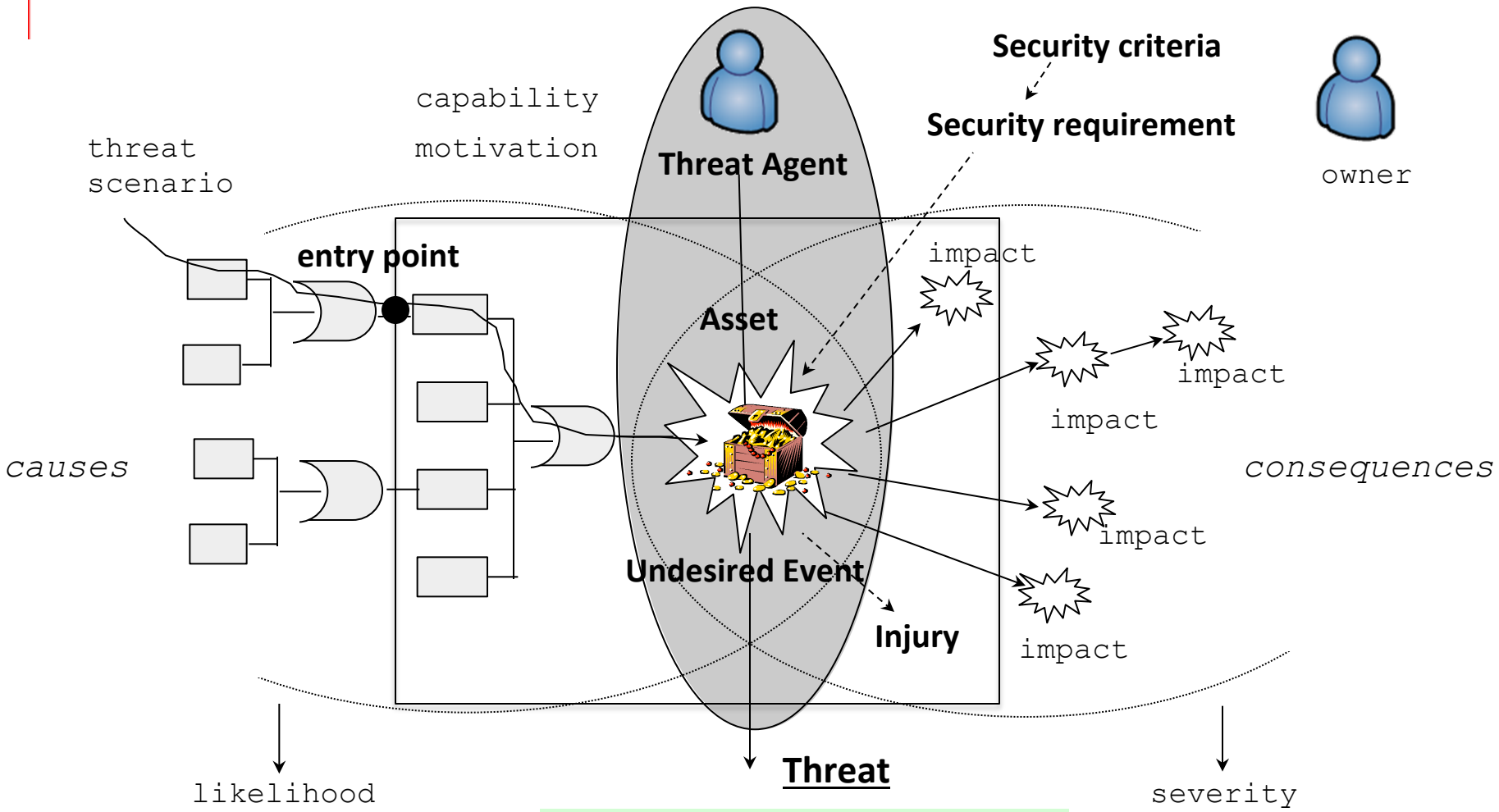
How do we exchange knowledge of "risk" ?

- "Risk" is not a *thing*, it is a complex statement [assertion] describing relations between many things

$$\text{Risk} = \int_{\text{Threats}} (\text{severity, likelihood})$$

- "Threat" is not a *thing* either, it is a complex statement describing relations between many things
- Therefore exchanging "risks" or "threats" is an utopia
  - But we can exchange elementary things and their relationships as facts

Fact-oriented threat and risk analysis



Risk = ∫ (severity, likelihood)

Threats